



Patent
42534-9300

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Natsume Matsuzaki

Serial No.: 09/544,069

Filed: April 6, 2000

For: MULTI-WORD ARITHMETIC
DEVICE FOR FASTER
COMPUTATION OF
CRYPTOSYSTEM CALCULATIONS

Patent Examiner: Mathhew Smithers

Group Art Unit: 2137

RECEIVED

SEP 22 2004

September 17, 2004

Technology Center 2100

Irvine, California 92614

TRANSMITTAL OF PRIORITY DOCUMENT

MAIL STOP AMENDMENT

Commissioner for Patents

PO Box 1450

Alexandria, VA 22313-1450

Dear Sir:

Enclosed is the certified copy of the priority document Japan 11-099657, for the above-identified patent application in accordance with 35 USC §119.

Please acknowledge receipt of this priority document.

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450 on September 17, 2004 by James Lee

Signature

Date of Signature: September 17, 2004

Very truly yours,

SNELL & WILMER LLP

Julio Loza, Reg. No. 47,758
1920 Main Street, Suite 1200
Irvine, CA 92614
949/253-4924

Notice (Mansu-paku) of ad.

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

52172-9800

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1999年 4月 7日

出願番号

Application Number:

平成11年特許願第099657号

出願人

Applicant(s):

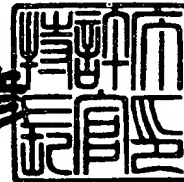
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 3月31日

特許庁長官
Commissioner,
Patent Office

近藤隆彦



出証番号 出証特2000-3022974

【書類名】 特許願

【整理番号】 2022510153

【提出日】 平成11年 4月 7日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 松崎 なつめ

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 奥村 康男

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 小野 貴敏

【特許出願人】

 【識別番号】 000005821

 【氏名又は名称】 松下電器産業株式会社

【代理人】

 【識別番号】 100097445

 【弁理士】

 【氏名又は名称】 岩橋 文雄

【選任した代理人】

 【識別番号】 100103355

 【弁理士】

 【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【プルーフの要否】 不要

【書類名】 明細書

【発明の名称】 多倍長演算装置

【特許請求の範囲】

【請求項 1】 複数種類の 1 ワード演算を処理する演算部と、
前記演算部の入出力データを格納するメモリ部と、
前記演算部の演算の種類と演算ワード数を指定して演算部を制御し、
さらに前記メモリ部のアドレスを指定する制御部からなる多倍長演算装置。

【請求項 2】 前記メモリ部から前記演算部に、1 ワードの入力データを少なくとも 2 つ同時に供給することを特徴とする請求項 1 記載の多倍長演算装置。

【請求項 3】 前記請求項 2 記載の前記メモリ部を少なくとも 2 つのサブメモリ部に分割し、各サブメモリ部から 1 ワードずつの入力データを、前記演算部に供給することを特徴とする請求項 2 記載の多倍長演算装置。

【請求項 4】 前記演算部は、乗算器とその出力を累算する加算器を含み、前記演算制御部の制御に応じて、乗算演算、または乗算とその結果の累算演算、または加算演算のいずれかを処理することを特徴とする請求項 1 記載の多倍長演算装置。

【請求項 5】 前記制御部は、前記演算部とメモリ部を用いた所定のシーケンス処理を制御することを特徴とする請求項 1 記載の多倍長演算装置。

【請求項 6】 前記メモリ部に、前記演算部からの入出力データを一時格納し、また前記制御部からのアドレス制御を一時格納する、メモリ入出力部を追加したことを特徴とする請求項 1 記載の多倍長演算装置。

【請求項 7】 前記メモリ入出力部を介して、外部からメモリ部への直接の書き込みと読み出しを可能とすることを特徴とした請求項 6 記載の多倍長演算装置。

【請求項 8】 前記メモリ部に格納されている各 n ワードの第 1 の入力 A 、第 2 の入力 B と法 P を入力として、前記演算部で $A+B-P$ の演算を行い、その結果の桁上げ信号を前記制御部に入力し、前記制御部において前記桁上げ信号が 1 のときは前記演算部の結果を前記メモリに格納し、0 のときに演算部の結果に法 P を加算したものを前記メモリに格納するように制御することにより、加算剰余演算を

行うことを特徴とする請求項 1 記載の多倍長演算装置。

【請求項 9】 1 ワードを k ビット、 R を $(k \times n + 1)$ ビットの値 $2^k (k \times n)$ としたとき、前記メモリ部に格納されている 2^n ワードの入力 A 、 n ワードの法 P を入力として、 P を法とした剰余体における $A \times R^* (-1)$ の値を求めてモンゴメリリダクション演算を行う多倍長演算装置であって、

前記メモリ部に、予め n ワードの $V = -P^* (-1) \bmod R$ の値を求めて格納しておき、前記演算制御部が、前記演算部で、前記 A の下位 n ワードと前記 V の部分積を最下位ワードから桁を合わせて順次加算し、下位 n ワードまでを求めて、その結果を中間値 B として前記メモリ部に格納する第 1 の乗算制御と、

前記中間値 B と前記法 P の部分積を最下位ワードを 0 ワード目としたとき、 $n - 2$ ワード目から桁を合わせて順次加算し 2^{n-1} ワード目までを求めて、その結果の上位 $n + 1$ ワードを中間値 C として前記メモリ部に格納する第 2 の乗算制御と、

前記 A の上位 $n + 1$ ワードを中間値 D として、

前記中間値 C と中間値 D の最下位ワードを加算したときの 1 ビットの桁上げ信号と、加算結果の 1 ワードがゼロでないときに 1 がセットされ、ゼロのときに 0 がセットされる 1 ビットのノンゼロ信号を出力する信号生成部と、

前記中間値 C と中間値 D の上位 n ワード、および前記各 1 ビットの桁上げ信号とノンゼロ信号を加算する加算制御と、

前記加算結果が前記法 P より大きい場合に、 P 以下になるまで前記加算結果より P を減算する減算制御を備え、

前記減算結果をモンゴメリリダクションの結果として前記メモリ部に格納することを特徴とした請求項 1 記載の多倍長演算装置。

【請求項 10】 前記信号生成部と加算制御部が、前記演算部において、前記各 $n + 1$ ワードの中間値 C と中間値 D に 1 ワードのオール 1 の値 $(2^k - 1)$ を加算して、加算結果の上位 n ワードを出力することを特徴とする請求項 9 記載の多倍長演算装置。

【請求項 11】 前記加算制御と減算制御を、請求項 8 記載の加算剰余演算制御により実現する請求項 9 記載の多倍長演算装置。

【請求項 12】 前記第 1、第 2 の乗算制御は、その出力部分積の m ワード目

は、 n ワードの第1の被乗数の i ワード目と第2の被乗数の j ワード目を、 $i+j=m$ を満たすようにすべての組み合わせで選んで、それぞれを前記演算部に入力して結果を累算することを特徴とした請求項9記載の多倍長演算装置。

【請求項13】 前記出力部分積の m ワード目の最終の累積結果を前記メモリに格納すると同時に、前記累算結果の上位にあふれた値を初期値とした、 $m+1$ ワード目の累算に対応した被乗数の前記メモリ部から前記演算部への読み出しを行うことを特徴とした請求項12記載の多倍長演算装置。

【請求項14】 前記第1の被乗数の i ワード目と第2の被乗数の j ワード目をメモリから前記演算部に呼び出して部分積を求めるのと同時に、出力部分積の m ワード目の部分累算結果を前記メモリから呼び出して、前記部分積と桁を合わせて加算し、同時に加算結果に対応する桁のメモリ部に格納することを特徴とした請求項12記載の多倍長演算装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、暗号演算などに用いられる多倍長の剰余演算装置に関し、特に楕円曲線暗号のように種々の演算を決められたシーケンスで行う場合に適している。

【0002】

【従来の技術】

従来、RSA暗号の演算装置として、乗算器とメモリからなる専用の演算装置が製品化されている。これは長語長のべき乗剰余演算処理だけを対象として、短いビット幅の乗算器を繰り返し用いて実現するものであり、CPUと組み合わせてコプロセッサとして用いる。

【0003】

これに対し、近年RSA暗号の次の公開鍵暗号として注目を集めているのが楕円曲線暗号である。この暗号方式は、RSA暗号では可能であった強力な攻撃法（Index Calculus法）が通用しないことにより、RSA暗号に比べ非常に短い鍵データ長であっても十分な安全性が確保できる。RSA暗号が1024ビット鍵で達成できる安全性を、楕円曲線暗号では160ビット鍵で確保する。しかし、一方、楕円曲線暗

号ではRSA暗号が基本的にべき乗剰余演算だけであったのに対し、四則演算他種々の演算が必要となり、またあらかじめ決まってはいるが条件分岐を含む複雑な手順での演算が必要になる。この楕円曲線暗号を従来のRSA暗号専用のコプロセッサを用いると、コプロセッサの演算はわずかとなり、ほとんどがCPUを用いた演算になってしまい、CPUとコプロセッサの制御の行き来によるオーバーヘッドが大きくなり高速処理が実現できない。

【0004】

また、全部をCPUソフトで実現すると、実装されるメモリの制限上、演算部に効率的にデータが供給できず、高速処理が実現できない。

【0005】

【発明が解決しようとする課題】

そのため、本発明では、楕円曲線処理に必要な種々の演算を、共通の演算部を兼用してこれを絶え間なく動作するようにメモリ部からデータを供給する。これにより回路規模を抑えながら楕円曲線暗号処理に必要な、種々の多倍長演算を効率的に実施することを目的とする。

【0006】

また、1つの演算部を繰り返し用いて多倍長の演算を行うため、演算幅の増減に柔軟に対応できる。繰り返し回数を増加することにより、ハード変更なしで安全性を高めることができる。

【0007】

【課題を解決するための手段】

本発明の第1の構成における多倍長演算装置は、
複数種類の1ワード演算を処理する演算部と、
前記演算部の入出力データを格納するメモリ部と、
前記演算部の演算の種類と演算ワード数を指定して演算部を制御し、さらに前記メモリ部のアドレスを指定する制御部からなることを特徴とする。

【0008】

本発明の第2の構成における多倍長演算装置は、第1の構成における前記メモリ部から前記演算部に、1ワードの入力データを少なくとも2つ同時に供給する

ことを特徴とする。

【0009】

本発明の第3の構成における多倍長演算装置は、第2の構成における前記メモリ部を少なくとも2つのサブメモリ部に分割し、各サブメモリ部から1ワードずつの入力データを、前記演算部に供給することを特徴とする。

【0010】

本発明の第4の構成における多倍長演算装置は、第1の構成における、前記演算部が、乗算器とその出力を累算する加算器を含み、前記演算制御部の制御に応じて、乗算演算、または乗算とその結果の累算演算、または加算演算のいずれかを処理することを特徴とする。

【0011】

本発明の第5の構成における多倍長演算装置は、第1の構成における、前記制御部が、前記演算部とメモリ部を用いた所定のシーケンス処理を制御することを特徴とする。

【0012】

本発明の第6の構成における多倍長演算装置は、第1の構成における、前記メモリ部に、前記演算部からの入出力データを一時格納し、また前記制御部からのアドレス制御を一時格納する、メモリ入出力部を追加したことを特徴とする。

【0013】

本発明の第7の構成における多倍長演算装置は、第6の構成における、前記メモリ入出力部を介して、外部からメモリ部への直接の書き込みと読み出しを可能とすることを特徴とする。

【0014】

本発明の第8の構成における多倍長演算装置は、第1の構成における、前記メモリ部に格納されている各 n ワードの第1の入力 A 、第2の入力 B と法 P を入力として、前記演算部で $A+B-P$ の演算を行い、その結果の桁上げ信号を前記制御部に入力し、前記制御部において前記桁上げ信号が1のときは前記演算部の結果を前記メモリに格納し、0のときに演算部の結果に法 P を加算したものを前

記メモリに格納するように制御することにより、加算剰余演算を行うことを特徴とする。

【0015】

本発明の第9の構成における多倍長演算装置は、第1の構成において、

1ワードを k ビット、 R を $(k \times n + 1)$ ビットの値 $2^k (k \times n)$ としたとき、前記メモリ部に格納されている $2n$ ワードの入力 A 、 n ワードの法 P を入力として、 P を法とした剰余体における $A \times R^{-1} \pmod{R}$ の値を求めてモンゴメリリダクション演算を行う多倍長演算装置であって、

前記メモリ部に、予め n ワードの $V = -P^{-1} \pmod{R}$ の値を求めて格納しておき、前記演算制御部が、

前記演算部で、前記 A の下位 n ワードと前記 V の部分積を最下位ワードから桁を合わせて順次加算し、下位 n ワードまでを求めて、その結果を中間値 B として前記メモリ部に格納する第1の乗算制御と、

前記中間値 B と前記法 P の部分積を最下位ワードを0ワード目としたとき、 $n-2$ ワード目から桁を合わせて順次加算し $2n-1$ ワード目までを求めて、その結果の上位 $n+1$ ワードを中間値 C として前記メモリ部に格納する第2の乗算制御と、

前記 A の上位 $n+1$ ワードを中間値 D として、

前記中間値 C と中間値 D の最下位ワードを加算したときの1ビットの桁上げ信号と、加算結果の1ワードがゼロでないときに1がセットされ、ゼロのときに0がセットされる1ビットのノンゼロ信号を出力する信号生成部と、

前記中間値 C と中間値 D の上位 n ワード、および前記各1ビットの桁上げ信号とノンゼロ信号を加算する加算制御と、

前記加算結果が前記法 P より大きい場合に、 P 以下になるまで前記加算結果より P を減算する減算制御を備え、

前記減算結果をモンゴメリリダクションの結果として前記メモリ部に格納することを特徴とする。

【0016】

本発明の第10の構成における多倍長演算装置は、第9の構成における、

前記信号生成部と加算制御部が、前記演算部において、前記各 $n+1$ ワードの中

間値Cと中間値Dに1ワードのオール1の値 $(2^k) - 1$ を加算して、加算結果の上位nワードを出力することを特徴とする。

【0017】

本発明の第11の構成における多倍長演算装置は、第9の構成における、前記加算制御と減算制御を、請求項8記載の加算剰余演算制御により実現する。

【0018】

本発明の第12の構成における多倍長演算装置は、第9の構成における、前記第1、第2の乗算制御は、その出力部分積のmワード目は、nワードの第1の被乗数のiワード目と第2の被乗数のjワード目を、 $i+j=m$ を満たすようにすべての組み合わせで選んで、それぞれを前記演算部に入力して結果を累算することを特徴とする。

【0019】

本発明の第13の構成における多倍長演算装置は、第12の構成における、前記出力部分積のmワード目の最終の累積結果を前記メモリに格納すると同時に、前記累算結果の上位にあふれた値を初期値とした、 $m+1$ ワード目の累算に対応した被乗数の前記メモリ部から前記演算部への読み出しを行うことを特徴とする。

【0020】

本発明の第14の構成における多倍長演算装置は、第12の構成における、前記第1の被乗数のiワード目と第2の被乗数のjワード目をメモリから前記演算部に呼び出して部分積を求めるのと同時に、出力部分積のmワード目の部分累算結果を前記メモリから呼び出して、前記部分積と桁を合わせて加算し、同時に加算結果に対応する桁のメモリ部に格納することを特徴とする。

【0021】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を用いて説明する。

【0022】

まず、一例として楕円曲線暗号の演算などに用いられる加算剰余演算の場合で

本発明を説明する。図1に多倍長演算装置の構成を示す。1は1ワードの演算部、2は加算剰余演算の対象となるデータを格納するメモリ部である。ここで1ワードとは処理の単位となるビット長であり、一般には16ビットや32ビットとなる。メモリ部は2つのサブメモリ部3と4に分かれており、それぞれ1タイミングに2つの1ワードデータを書き込み、または読み出しできるものとする。5は演算部やメモリ部の入出力を一時蓄えるためのメモリ入出力部である。メモリ入出力部を介して、外部よりメモリ部へデータの入出力も行う。また6は演算部を制御し、またメモリ入出力部にアドレスを供給する制御部である。

【0023】

図2に演算部の構成例を示す。10は3入力加算器、11は結果を蓄えるレジスタ(Reg)である。演算部には3つのそれぞれ1ワードのデータが同時に入力され、また同時にレジスタ11に蓄えられている前タイミングでの演算結果が出力される。

【0024】

以下では、この多倍長演算装置を用いて5ワードの加算剰余演算を行う際の手順を説明する。5ワードの値を、例えば $A=(a_4, a_3, a_2, a_1, a_0)$ のように表す。 a_4, \dots, a_0 はそれぞれ1ワードで、 a_4 が最上位、 a_0 が最下位の1ワードとする。2つの入力を $A=(a_4, a_3, a_2, a_1, a_0)$ 、 $B=(b_4, b_3, b_2, b_1, b_0)$ とし、法を $P=(p_4, p_3, p_2, p_1, p_0)$ としたとき、加算剰余演算は、 $C=(c_4, c_3, c_2, c_1, c_0) = A + B \bmod P$ を求めるものとする。ここで、 $\bmod P$ は P で除したときの剰余を示す。

【0025】

図3にメモリ1およびメモリ2のメモリマップを示す。メモリ1には入力 A と P 、メモリ2には入力 B と出力 C および、ワーク領域 W が配置される。それぞれ最下位ワードから順に格納される。入力データ A 、 B 、 P の格納は図1におけるメモリ入出力部を介して外部から行うとよい。また出力 C についてもメモリ入出力部を介して外部に読み出すとよい。なお、ここでの外部とは例えばホストCPUの内部メモリとする。

【0026】

このメモリを用いた加算剰余演算の処理手順を図4に示す。まず、図2に示す

Reg 1 1 および Carry 入力を 0 に設定して、メモリ 1 から入力 A の最下位 a_0 、メモリ 2 から入力 B と P の最下位 b_0 、 p_0 をそれぞれ同時に演算部に入力する。そして、図 2 に示す 3 入力加算器で、 $a_0 + b_0 - p_0$ の演算を行い、結果を Reg 1 1 に格納する。次に、次の桁の a_1 、 b_1 、 p_1 をメモリから獲得して前の桁のキャリーを含めた加算演算をするのと同時に Reg に格納されている前の桁の結果をメモリ 2 の w_0 に格納する。メモリ 1 からは a_1 、 p_1 の読み出し、メモリ 2 からは b_1 の読み出しと、 w_0 の書き込みが 1 タイミングに同時に行われる。なお、各メモリは 1 タイミングに 2 つのデータをアクセスできるものとしている。

【0027】

以降同様にして、 $W = A + B - P$ の演算を行う。この結果、桁上げ信号 carry が 0 になったときは（図 4 における左側のルート）、 $A + B$ の結果が P 未満であったことを示すため、結果に P を加えて引き戻す。桁上げ信号は演算部から制御部に通知されて、制御部において分岐を伴ったシーケンス制御がなされる。W と P の加算演算は、メモリ 1 の法 P とメモリ 2 の W 領域の最下位ワードから 1 ワードずつ演算器に入力し、1 つ前の結果をメモリ 2 の C に同時に格納することにより実施する。メモリ 1 は同時に 1 回だけアクセス、メモリ 2 は読み出しと書き込みの計 2 回アクセスする。また、桁上げ信号 carry が 1 のときは（図 4 における右側のルート）、W の結果をそのまま出力の領域 C に格納する。この場合はメモリ 2 のみを読み出しと書き込みの計 2 回アクセスする。

【0028】

また、別の例としてモンゴメリ方式を実現する本発明の説明する。モンゴメリ方法は、暗号演算で多用される剰余演算を高速に行う方法である。詳細は例えば、岡本龍明・太田和夫共編「暗号・ゼロ知識証明・数論」共立出版、1995年、を参考にすることにし、ここでは演算の概要だけを説明する。以下は、 $P < R = 2^m$ とし、 P 2 程度の大きさの A に対して、 $M = A \cdot R - 1 \bmod P$ を求める、モンゴメリリダクションと呼ばれている処理である。

【0029】

入力：A（ $2m$ ビット程度の値）

前計算： $V = -P^{-1} \bmod R$

出力: $M = A \cdot R - 1 \pmod{P}$

処理:

step1: $B = A \times V \pmod{R}$

step2: $M = (B \times P + A) / R$

step3: $M \pmod{P}$ を出力

図1の多倍長演算装置の構成を用いる。図5にモンゴメリ演算の場合の演算部の構成を示す。この演算部は、1ワード幅の乗算器を備え、乗算結果を加算器で累算する。制御により加算器としても用いることができ、先に述べた例の加算剰余演算も実現できる。

【0030】

以下では、上記step1-3の各処理の実現について順次説明する。なお、以下の説明では、 P 、 V がそれぞれ5ワード、 A が10ワードの場合について説明する。

【0031】

[step1]

A の下位5ワードと V の積を桁を合わせて最下位から累算し、下位5ワードまで求める。 \pmod{R} をとっているために、それより上位は求める必要がない。例えば、メモリ1に格納した A の下位5ワード $= (a_4, a_3, a_2, a_1, a_0)$ と、メモリ2に格納した $V = (v_4, v_3, v_2, v_1, v_0)$ を乗算して、メモリ1の B 領域に格納する場合について説明する。図6では、5ワードの A と V の積を筆算の要領で部分積を桁を合わせて累積することにより求める様子を示している。

【0032】

(1) まず、 a_0 と v_0 を同時に2つのメモリから読み出して、図5の乗算器に入力する。結果の下位1ワード分をメモリ1の b_0 に格納し、それより上位は1ワード分シフトダウンして、加算器の一番右の入力に設定する。

【0033】

(2) 次に、 a_1 と v_0 を同時に2つのメモリから読み出して、乗算して結果を加算器で累算する。なお、このメモリ読み出しと(1)における b_0 の格納を同時に行うと、処理時間が削減できる。また a_0 と v_1 を乗算して結果を加算器で累算する。なお、この2つの部分積は桁が一致しており、2つの被乗数の添え字の数字を加算

すると1になる。これらの結果の下位1ワード分をメモリ1のb1に格納し、それより上位は1ワード分シフトダウンして、加算器の一番右の入力に設定する。

【0034】

(3) 次に、桁が一致している、a2とv0の乗算と累算、a1とv1の乗算と累算、a0とv2の乗算と累算を行う。なお、このメモリ読み出しと(2)におけるb1の格納を同時に行うと、処理時間が削減できる。また、この桁では、2つの被乗数の添え字の数字を加算すると2になる。累算の結果の下位1ワード分をb2に格納し、それより上位は1ワード分シフトダウンして、加算器の一番右の入力に設定する。

【0035】

以下同様に作業を続ける。なお、この例では、下位mビットは5ワード分となる。そのため、2つの被乗数の添え字の数字の和が4になる桁までを求めればよい。結果を $B=(b_4, b_3, b_2, b_1, b_0)$ とする。なお、最後に演算部のレジスタに残った、5ワードより上位の値は切り捨てる。

【0036】

[step2]

$B \times P$ の演算も、step1と同様に部分積を累算する方法で行う。ただし、この場合はAとの加算も行い、その結果の上位mビットが必要になる。step1の場合と同様に、B、Pが5ワード、Aが10ワードの場合で手順を説明する。図7では、筆算の要領で部分積を桁を合わせながら累積する様子を示している。

【0037】

まず、BとPの被乗数の添え字の和が3となる桁から部分積を求め、最後の $b_4 * v_4$ の桁までの積を桁をそろえて累算する。累算結果のうち最下位ワードを除いた6ワード分をCとする。またAのうち、このCと桁を合わせた上位6ワードをDとする。

【0038】

CとDの最下位ワード(図7においてハッチング)に着目し、これらを加算したときの1ビットの桁上げ信号を求める。また、加算結果の1ワードがゼロでないときに1がセットされ、ゼロのときに0がセットされる、ノンゼロ信号も求める。そして、CとDの最下位ワードを除いた各5ワード、および前記桁上げ信号と

ノンゼロ信号の和を求め、これを出力Mとする。つまり、前記桁上げ信号とノンゼロ信号により、CとDの最下位ワードを除いた各5ワードの和に、

- ・ 桁上げ信号 = 0、ノンゼロ信号 = 0 のとき、 0
- ・ 桁上げ信号 = 0、ノンゼロ信号 = 1 のとき、 1
- ・ 桁上げ信号 = 1、ノンゼロ信号 = 0 のとき、 1
- ・ 桁上げ信号 = 1、ノンゼロ信号 = 1 のとき、 2

が加算され、出力Mとなる。

【 0 0 3 9 】

勿論この加算についても演算部内の1ワード幅の加算器を繰り返し用いるものとする。

【 0 0 4 0 】

なお、上位mビットの出力Mを、部分積を最下位から全部順番に求めず、n-2ワード目より上位だけを用いて求めている。そのため、高速化が実現できている。

【 0 0 4 1 】

なお、上記桁上げ信号とノンゼロ信号を生成してから出力Mを求める代わりに次のようにしてMを求めることも出来る。

【 0 0 4 2 】

前記6ワードのCとDと、その最下位ワードの位置に1ワードの各ビットに1をセットした値（オール1と呼ぶことにする）を加算する。そして、その結果の上位5ワードをMとする。この方法では、桁上げ信号やノンゼロ信号を生成する部分を設けなくても、図5で示した演算器を利用することにより実現できるため、回路規模の面より有利である。

【 0 0 4 3 】

以上の処理により、BとPの部分積のうち例えば $b_0 \cdot p_0$ 、 $b_1 \cdot p_0$ などの添え字の和が2以下の部分積は求めなくてもよく、処理速度の高速化が実現できる。また、桁が変わる毎にその桁の結果をメモリに格納するが、この格納と次の桁の読み出しを同時に処理するために、演算部は休みなく動作することができる。

【 0 0 4 4 】

[step3]

Mの値を法P以下になるまでPを減算する。この減算についても演算部内の1ワード幅の加算器を繰り返し用いて、その最上位ワードからのキャリー出力により、P以下になることを確認する。

【0045】

なお、以上の説明ではmビットを5ワードとしたが、これに限定されるものではない。例えば楕円曲線暗号で用いる場合にはmは160程度、RSA暗号の場合には1024程度になる。

【0046】

また、図1における構成では演算部とメモリ部のタイミングを取るため、および外部からメモリ部に直接アクセスするために、メモリ入出力部を設けたが、必要のない実装もある。

【0047】

また、図1における構成ではメモリ1、2がそれぞれ独立のメモリであり、1タイミングに2回アクセスできるようなものとしたが、これを実現するためメモリ部だけに2倍の周波数のクロックを与えてもよい。またデュアルポートメモリを用いてもよい。

【0048】

【発明の効果】

以上のように本発明によれば、楕円曲線暗号に必要な種々の多倍長演算を、小さなハードで高速に処理できる。また繰り返し回数を制御するだけで、ハード自身は変更することなく安全性を向上することができる。またメモリ部をうまく配置実現することにより、演算部を休みなく動作させて、処理の高速化が実現できる。

【0049】

また、本発明の多倍長演算装置を用いて、楕円曲線暗号で必要となる加算剰余演算と、モンゴメリリダクション演算の処理シーケンスを制御することにより、それぞれの処理における演算部の繰り返し回数が削減できる。

【図面の簡単な説明】

【図1】

本発明の一実施形態における多倍長演算装置の構成例を示す図

【図 2】

本発明の一実施形態である加算剰余演算における演算部の構成例を示す図

【図 3】

本発明の一実施形態である加算剰余演算におけるメモリ部のマップを示す図

【図 4】

本発明の一実施形態である加算剰余演算における処理フローチャート

【図 5】

本発明の一実施形態であるモンゴメリリダクションにおける演算部の構成例を示す図

【図 6】

本発明の一実施形態であるモンゴメリリダクションにおけるstep1の処理を説明した図

【図 7】

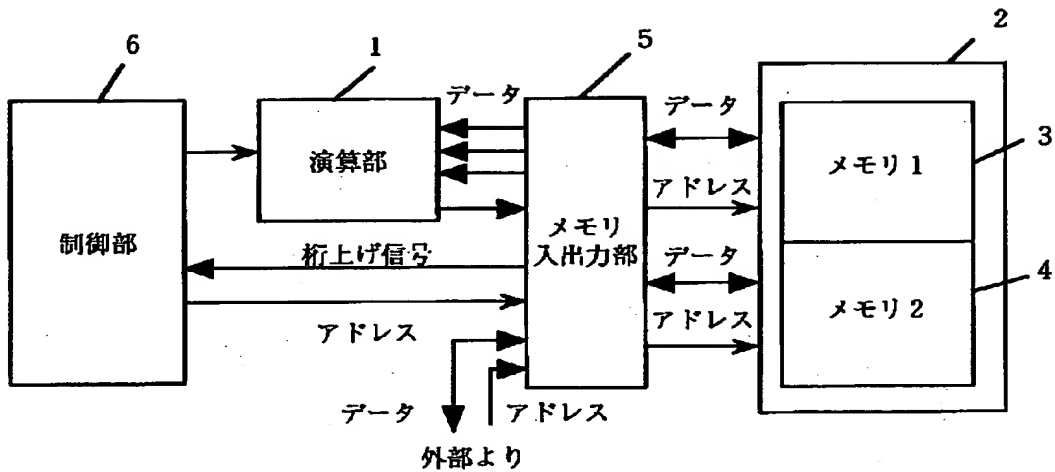
本発明の一実施形態であるモンゴメリリダクションにおけるstep2の処理を説明した図

【符号の説明】

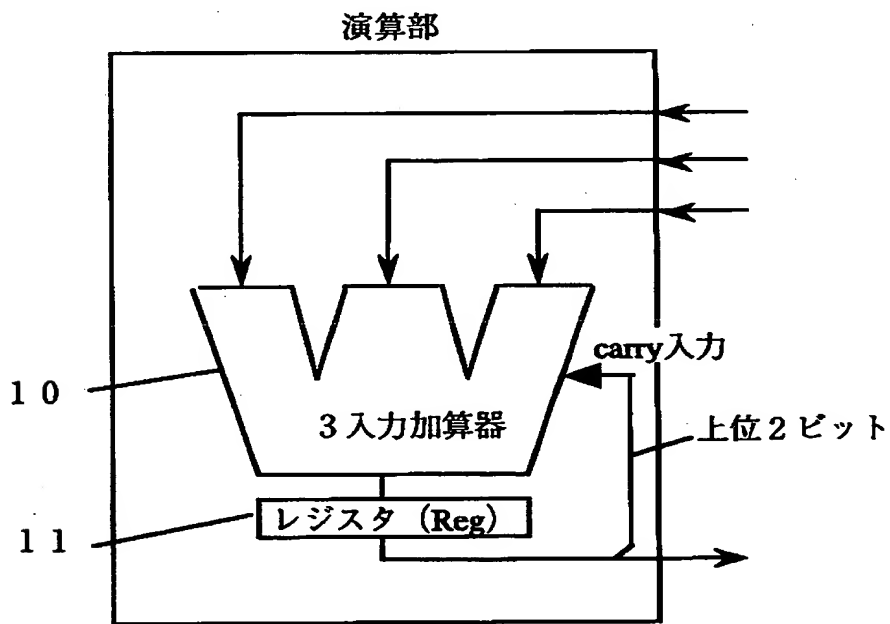
- 1 演算部
- 2 メモリ部
- 3 サブメモリ 1
- 4 サブメモリ 2
- 5 メモリ入出力部
- 6 制御部
- 10 3入力加算器
- 11 レジスタ

【書類名】 図面

【図 1】



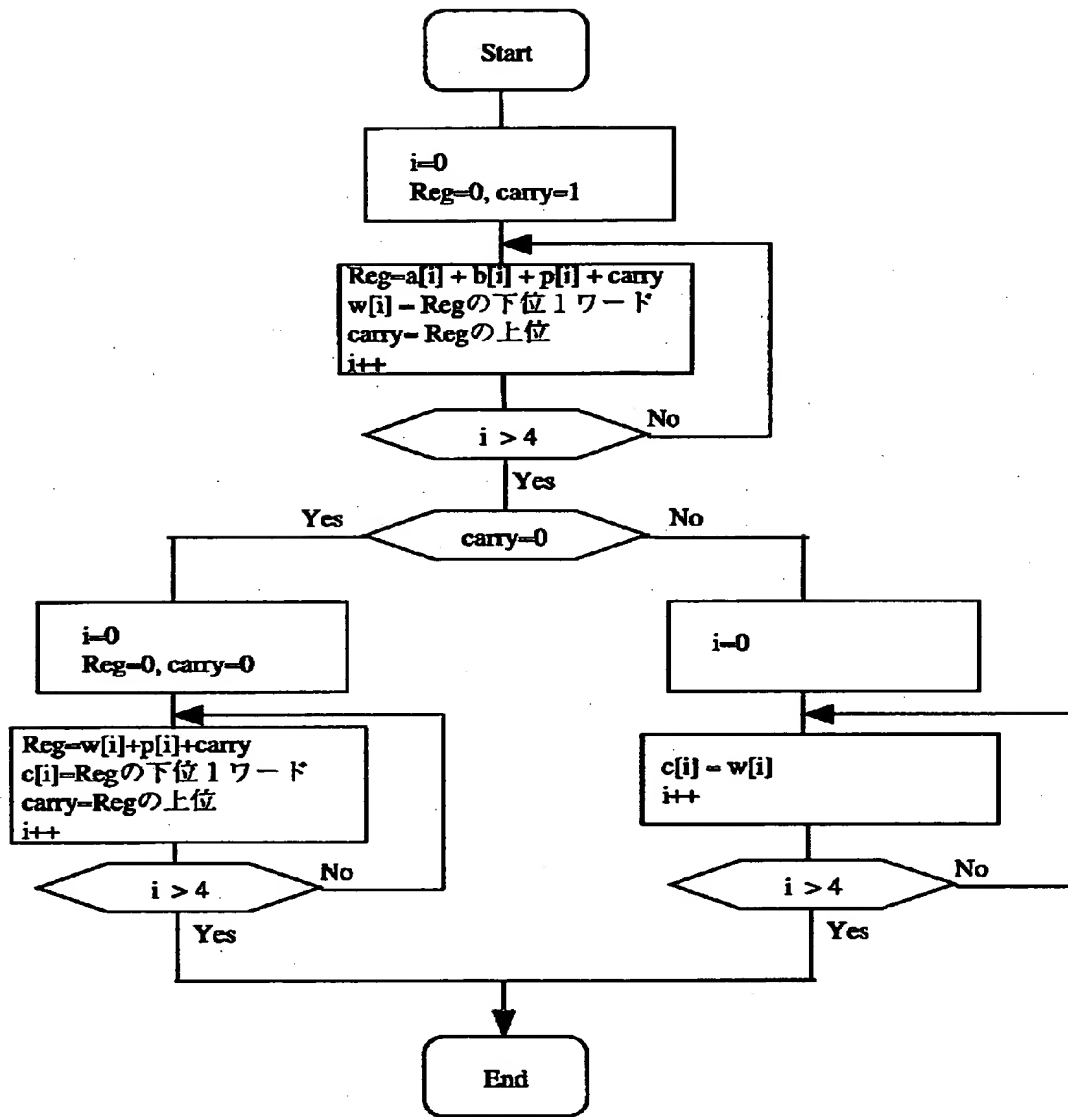
【図 2】



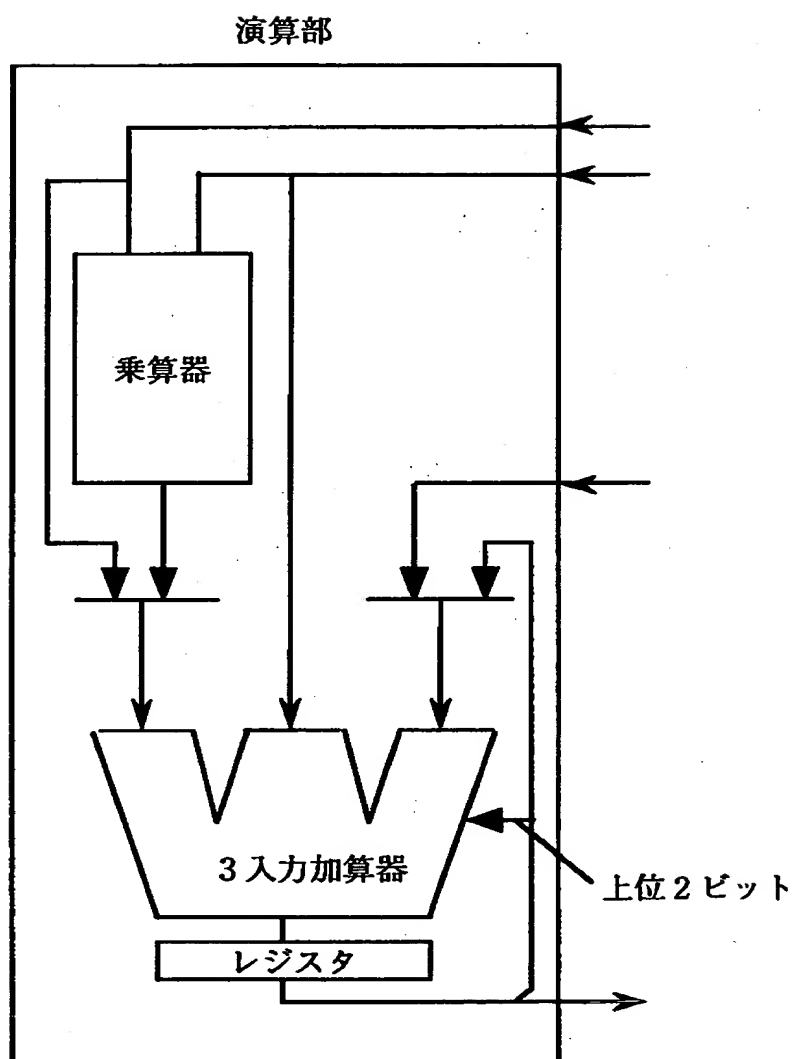
【図 3】

メモリ 1		メモリ 2	
a0		b0	
a1		b1	
a2		b2	
a3		b3	
a4		b4	
⋮		⋮	
p0		c0	
p1		c1	
p2		c2	
p3		c3	
p4		c4	
		⋮	
		w0	
		w1	
		w2	
		w3	
		w4	

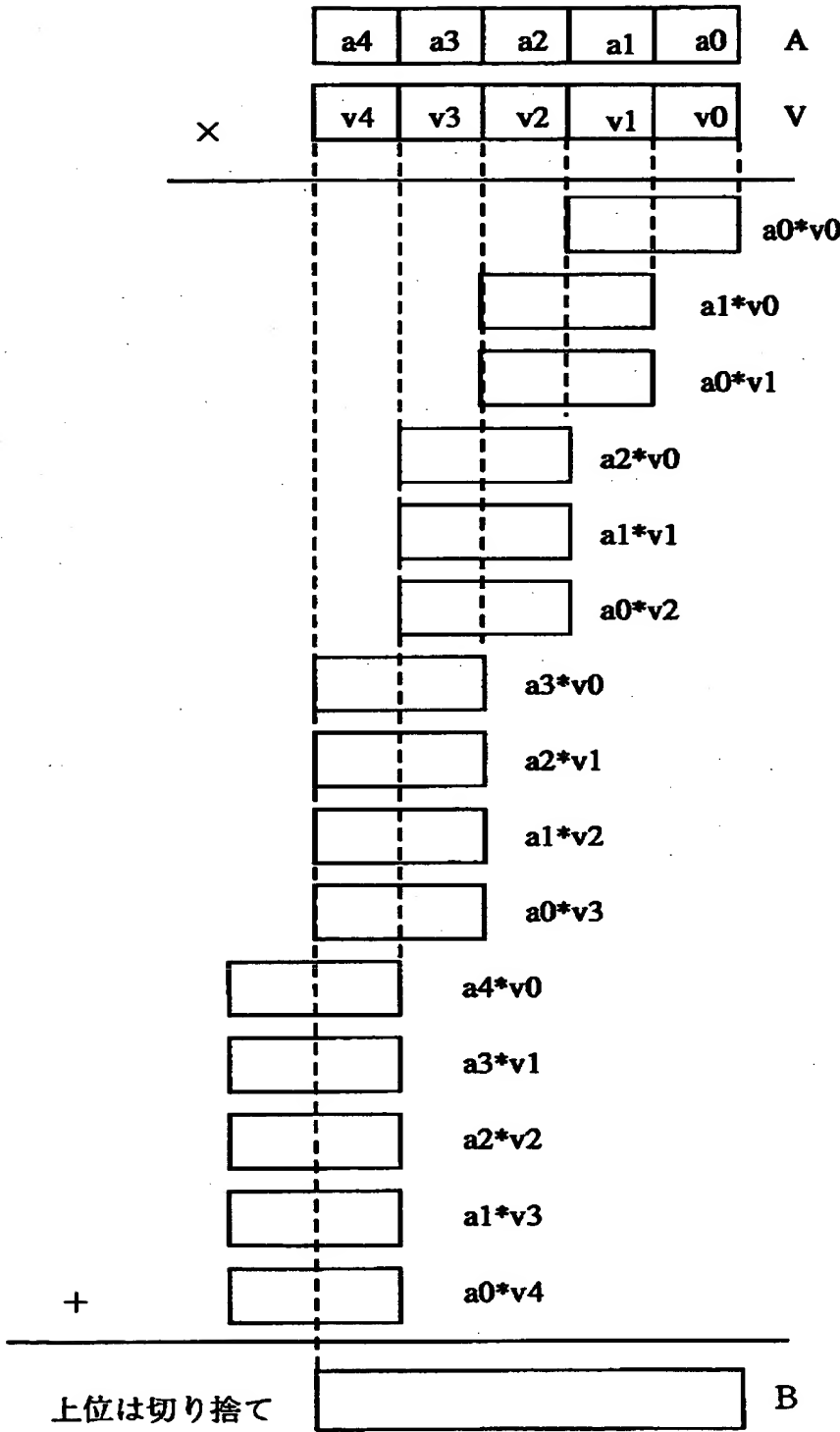
【図 4】



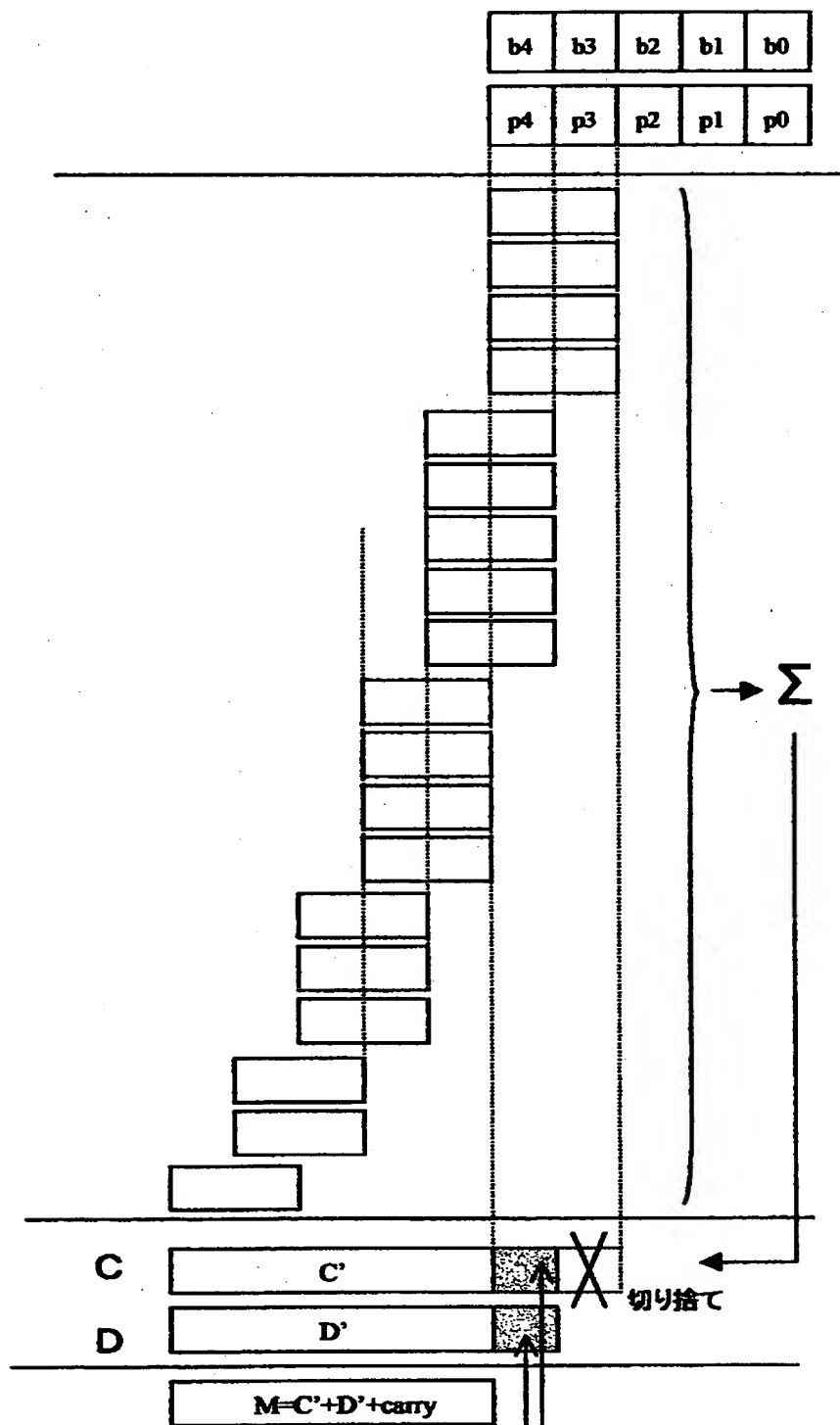
【図 5】



【図 6】



【図 7】



加算して、
 上位への桁上げが0で和が0のとき, carry=0
 上位への桁上げが1で和が0のとき, carry=1
 上位への桁上げが0で和が0でないとき, carry=1
 上位への桁上げが1で和が0でないとき, carry=2

【書類名】 要約書

【要約】

【課題】 楕円演算のような複雑な演算を、小さなハードウェアで高速に実現する。制御を加えることにより楕円演算とRSA暗号演算が切り替えて実現できる。

【解決手段】 演算部とメモリ部と制御部からなる。演算部に効率的にデータを供給するメモリ部の構成とその制御方法が発明のポイント。加算剰余演算 ($A+B \bmod P$) では、演算部は3入力加算器からなり、入力A、B、法Pを同時に入力して、 $A+B-P$ の計算を行う。この桁上げ信号により制御シーケンスを変更し、結果が負となる場合には、Pを加算して、最終的に $A+B \bmod P$ を求める。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地
氏 名 松下電器産業株式会社